



Business Case Analysis

INVESTING IN A STATEWIDE INFORMATION SECURITY AND PRIVACY OFFICE (SISPO)

March 2007

**Presented to Government Information Technology Agency (GITA)
State of Arizona**

Prepared by Coalfire Government Systems, LLC.

Project Manager
Harley Rinerson
harley.rinerson@coalfiresystems.com
(303) 554-6333

Table of Contents

1. EXECUTIVE SUMMARY	3
2. STATUS OF ARIZONA IT SECURITY AND PRIVACY.....	8
3. INFORMATION RISK OVERVIEW	11
4. WHY SISPO IS A BEST PRACTICE.....	14
5. SISPO COMPONENTS AND RESPONSIBILITIES	15
6. INDEPENDENT RISK ASSESSMENT.....	20
7. SUMMARY of SISPO FUNCTIONS.....	23
8. FUTURE FUNCTIONS.....	37
9. CONCLUSION	38
APPENDIX A: CONSULTANT QUALIFICATIONS and PROJECT METHODOLOGY.....	39
APPENDIX B: ACRONYMS AND ABBREVIATIONS.....	41
APPENDIX C: GLOSSARY OF TERMS	44
APPENDIX D: REFERENCES.....	46

1. EXECUTIVE SUMMARY

Purpose

In today's economic and political environment, addressing security has become a core necessity for government organizations since these organizations are primary repositories of trusted citizen data. As the State of Arizona obtains faster and more efficient service delivery from e-government and other technology initiatives the importance of secure and reliable data increases.

The State of Arizona is not prepared to mitigate known risks to State information system resources or to assure their citizens that controls have been effectively deployed to prevent data compromise. While the State has published comprehensive information security policies, the State does not coordinate comprehensive security plans or consistently enforce current security standards.

The purpose of this document is to identify the need for a Statewide Information Security & Privacy Office (SISPO) to be placed within Government Information Technology Agency (GITA) to mitigate increased risks from cyber threats.

This document identifies:

- SISPO best practices from around the United States
- The current condition of IT security in Arizona State government
- The key functions of an effective SISPO
- The rationale behind each such function, and
- The resources required for a successful SISPO for Arizona.

This report was prepared to help the State make an informed decision on risk mitigation benefits associated with establishing a SISPO within GITA for Arizona State government.

Background

The risks to mission critical State information systems and citizen privacy are well chronicled.

- **Lack of data protection is a national problem**
 - The U.S. Federal Trade Commission (FTC) reports that identity theft has become the number one consumer complaint processed over the past two years. Over 40% of all citizen complaints to the FTC are associated with data and privacy protection.
 - The ID Theft Resource Center reports identity theft as the ***“Nation’s Fastest Growing Crime”***.¹
 - Arizona has led the nation in Identity Theft for the ***fourth year in a row***.
 - Approximately one out of nine citizens have already received at least one notice of data compromise and, in a recent Ponemon study 80% of respondents fear that they will become a victim of identify theft.²

¹ http://www.idtheftcenter.org/factsandstats_1006.pdf

² 2006 Annual Study: Cost of a Data Breach, Ponemon Institute.

- **Government organizations are the largest contributors to this problem:**
 - The same report from the ID Theft Resource Center identified that **over 60% of all data breaches reported in 2006 were caused by university or government organizations.**
 - The Veterans Administration, where the sensitive personal data of 26.5 million veterans was placed at risk, has become the face for government indifference to data protection.
- **The cost of data breaches is significant.**
 - Data breach incidents cost organizations an average of \$182 per consumer or citizen record including over \$50 per record just to respond to the incident.
 - In a 2006 Internet Crime Report, the FBI's Internet Crime Complaint Center reported that cyber crime complaints cost over \$198.4 million.³ Many cyber crimes go unreported. Accordingly, the FBI has changed its priorities in the last few years to address cyber crime as its number two priority after counter terrorism.
 - Congress estimates that if the Veteran's Administration (VA) were to experience another data breach similar to the data theft that occurred on May 3, 2006 the cost could be as much as \$1 billion.⁴
 - The impact of data breach on individuals is disruptive and time consuming to remedy. In some cases, individuals cannot recover from identity theft.
- **Data breach risks can be significantly reduced through established national best practices.**
 - Arizona is lagging behind other States with 83% of States having already implemented a statewide Chief Information Security Officer or equivalent position to oversee their organization's security controls.⁵

Arizona is the identity-theft capital of the U.S. MSN Money, 2006

FTC Identity Theft Statistics for 2006

Top 10 states for identity theft (on per-capita basis)

Rank	State	Victims/100,000	Total victims
1	Arizona	147.8	9,113
2	Nevada	120.0	2,994
3	California	113.5	41,396
4	Texas	110.6	26,006
5	Florida	98.3	17,780
6	Colorado	92.5	4,395
7	Georgia	86.3	8,084
8	New York	85.2	16,452
9	Washington	83.4	5,336
10	New Mexico	82.9	1,621

Source: Federal Trade Commission

³ Internet Crime Report, January 1, 2006 – December 31, 2006, Internet crime Complaint Center, prepared by National White Collar Crime Center and the Federal Bureau of Investigation

⁴ U.S. Congressional Budget Office, Cost Estimate, H.R. 5835, Veterans Identity and Credit Security Act of 2006, July 28, 2006, p.1.

⁵ A Current View of the State CISO: A National Survey Assessment, September 2006, National Association of Chief Information Officers (NASCIO), p.1.

- The August 2006 Ponemon study identifies a “lack of accountability” by organizations responsible for data as the root cause for most data incidents.
- **Toleration of unauthorized access and misuse of information by the public is decreasing.**
 - The Veteran’s Administration learned a valuable lesson. Had the VA only secured laptop computers for \$6 million prior to the incident, they would not have been at risk for \$16 million in notice of breach and credit monitoring costs alone plus an initial estimate of a total cost of \$500 million in related remedy and damage costs.⁶ The outrage experienced by the veterans who were victims of the VA incident was not based solely on the breach itself, but was heightened by the perceived indifference associated with the management of their sensitive data by a trusted government institution. Aside from the financial loss, the Veterans Administration has suffered a reputation loss that will impact confidence in their services for the foreseeable future.
 - The tolerance for unauthorized access and misuse of information about them is decreasing. Citizens expect proper stewardship by government entities that collect, process and store their sensitive personal data.

State of Arizona & IT Security

The current controls in place in State of Arizona government are insufficient by today’s standards, and create the potential for members of the public to become victims of identity theft along the lines of the Veteran’s Administration incident.

A June 2005 Auditor General report (05-03) confirmed that significant control deficiencies exist in the current Information Technology (IT) infrastructure and process. The **primary finding** was that “GITA, as the State’s information technology coordinator, **should take a stronger leadership role** in the State’s IT management operations in five key areas...” These included the need for GITA to do more to ensure that agencies **consistently adhere to security standards** and to **strengthen standards** it already has to **protect the privacy of data**; and that GITA should ensure that agencies comply with these standards. **The report says that GITA needs to develop a comprehensive security plan and should consider establishing a chief security officer.**

The most recent Technical Infrastructure Standards Assessment (TISA) submitted by State agencies to GITA indicates that the State is making progress in deploying controls to protect mission critical information resources and citizen privacy. However, other states have discovered a significant gap between self reported compliance and the results of independent assessments. Other states have found that agencies lack an in-depth understanding of the metrics for security reporting and the resources to truly measure compliance with statewide security standards. It is highly likely that the State of Arizona will also find similar over-reporting of compliance should a statewide independent risk

Impact of privacy data breach

- **330 hours spent on recovering from the crime over a period of years**
- **Higher cost for credit**
- **Inability to get a job**
- **Collection calls for fraudulent transactions**
- **Terrorist access to the US with fals identities**

Source: **Id Theft Resource Center,**
www.idtheftcenter.org

⁶ Testimony of Secretary of Veterans Affairs James Nicholson to a question in U.S. Congress, House Committee on Veterans Affairs, Hearing on the Recent Security breach at the Department of Veterans Affairs, in which 26.5 million Veterans Records were Stolen from the Home of a VA employee, 109th Cong., 2nd session. May 25, 2006.

assessment be conducted as we recommend.

Accordingly, the State is currently accepting risks and may face the following attendant consequences

- More frequent service disruption
- Lessened homeland security control
- Escalating financial and legal liability
- Erosion of citizen trust in government

For the State of Arizona, the cost for establishing an SISPO versus the impact of potential security breaches is highlighted below.

Estimated Cost of AZ Government Data Breach
If only 2% of State citizens are impacted by a breach, the following costs could be anticipated:
<u>6.5 M citizens x 2% x \$182 = \$ 23.6 million</u>
PLUS
Immeasurable loss of trust in State government

Conclusion

This business case justifies formal deployment of a State government SISPO within the Government Information Technology Agency (GITA).

Eighty-three percent (83%) of other States already have a statewide security office to provide expected oversight and governance.⁷ By providing the SISPO with adequate resources and authority, Arizona State officials and legislative members would be deploying “reasonable” oversight to enhance the protection of critical information resources as well as demonstrating due care in the management of this critical function.

Essentially, the SISPO would perform the strategic, planning, policy development and training functions required to reduce unjustified levels of risk. The SISPO would be an independent security and privacy governance and oversight function that would provide clear leadership for the development of a comprehensive security plan. To prepare agencies to consistently implement State policies and standards, the SISPO would facilitate training, planning and security implementation in the agencies. The agencies would remain responsible for their individual security programs but the SISPO would play an invaluable role in providing leadership and coordination for integrated and effective implementation of security and privacy plans.

**“The time has come
for Arizona to have a
dedicated information
security and privacy
office.”**

**- Chris Pierson
Lewis and Roca
President of Phoenix Chapter of
InfraGard**

It is strongly recommended that the State of Arizona formally establish the Statewide Information Security & Privacy Office within GITA and allocate sufficient resources to phase in operations over a

⁷ Ibid.

three year period. The office must write and own the Statewide Information Technology Security Strategic Plan and Program and maintain timely compliance oversight with the goal of institutionalizing information security and privacy statewide.

The SISPO would not replace or disrupt ongoing security operations performed within agencies or by the Department of Administration (ADOA) for shared services. In fact, the first phase should focus on completing a formal risk assessment and updating policies to guide consistent risk mitigation efforts within agencies. The second and third phases should institute policy enforcement, incident response reporting, and facilitate coordinated security planning among the agencies.

The SISPO would not only set the baseline standards, it would provide the transparency necessary for the Governor and legislature to respond to citizen inquiries before the next cyber incident occurs. When citizens ask, "What has the State been doing to protect our data?", the State's leaders will have a clear, supportable response.

2. STATUS OF ARIZONA IT SECURITY AND PRIVACY

While the State has published information security policies and standards, a 2005 Auditor General report (05-03) identified that “State agencies do not always adhere to the standards and, as a result, are potentially exposed to serious security threats.” The current state of information security within the State of Arizona is not fully known due to the lack of a comprehensive risk assessment and validated reporting on the effectiveness of current information security controls.

The 2006 Technology Infrastructure Standards Assessment (TISA) performed by GITA reports improvement in security programs within State agencies but no independent assurance testing has been conducted to validate agency self-reported improvements. Accordingly, neither the Executive nor members of the State legislature would be able to credibly answer the potential citizen call for an accounting of information security controls (deployed to protect personal data or other critical state information assets).

For information security, the lack of significant public incidents is not an indicator that all existing controls are operating effectively. The State does not, in contrast with best practices, maintain a central enforcement authority that has the ability to act on cross agency incidents or to track agency levels of incident response and lessons learned. The State also does not have a central organization with the resources to enforce inter or intra-agency incident reporting. Therefore, reliable data on the impact of failed controls is not readily available.

Data collected through interviews with selected State agencies revealed that localized controls in some agencies have been deployed and appear to be operating. However, current controls are not consistent, were not uniformly selected and were not justified through a comprehensive risk analysis process. Therefore, it is difficult to determine the probability of future incidents or to judge the capability of the State to currently respond to cyber incidents.

The Privacy Rights Clearinghouse web site reports that over 100 million consumer records may have been compromised in the last 18 months.⁸ The continuing increase in reported compromises nationally indicates that the State of Arizona remains at significant risk of a data compromise.

During the past quarter, our firm supported the forensic investigation of several incidents in another state. Those incidents ranged from a lost laptop to missing backup tapes to a cyber hack that could result in information theft or disruption of services. Due to recent laws that require consumer notice for breach of privacy, many citizens of that State received up to three notices on privacy breach within a month's time. The impact was significant. Those compromised citizens are telling many others and are demanding more responsible action to protect their data.

Since the State of Arizona notice of privacy breach legislation went into effect in September 2006, it is anticipated that increase visibility of data breaches will be forthcoming soon in Arizona as well.

“The advancement of e-commerce activities poses a rising security concern and increases potential liability for the State of Arizona.”

**- Debra Davenport
Auditor General**


⁸ <http://www.privacyrights.org>

The State of Arizona is comprised of approximately 110 state agencies, boards and commissions. To serve their specific needs, IT resources have been deployed in a decentralized structure. Larger agencies have acquired and deployed a higher level of security controls than small and medium size agencies. However there is no consistent implementation of the State's IT Security Standards across agencies. **The State agencies are interconnected through AZNet, the State's IT network, and accordingly, the entire State is only as strong as its weakest agency, board or commission in terms of security controls.**

In most cases, security controls have not been aligned with business requirements or justified by data sensitivity. While the State maintains an inventory of IT assets, IT management within agencies does not uniformly rate the criticality of those resources by confidentiality, integrity or availability metrics. Accordingly, ongoing security planning is conducted with institutional knowledge and individual preference rather than structured oversight and governance.

One of the largest gaps in the implementation of security controls is the lack of effective oversight. While the State has formed an Information Technology Security Advisory Committee (ITSAC) to raise awareness for cyber security within the State, the ITSAC does not have access to central resources to conduct risk assessments and recommend risk mitigation strategies to agencies that own the mission critical systems and data. Moreover, it does not have the resources to measure control effectiveness or recommend adjustments to the security program when threats or operating environments change. ITSAC has nonetheless proven resourceful and has provided significant value to all agencies in growing awareness for enhanced security controls. The ITSAC also endorses the recommendation to institutionalize statewide information security powers and responsibilities within a SISPO under GITA authority.

Our analysis of the current status of the State of Arizona Information Security Programs is subjective since the oversight and measurement of these programs has not yet been established. However, the sporadic deployment of sophisticated controls in some agencies would justify a "Level 2" rating for the entire enterprise in accordance with the metrics imposed by the National Institutes of Standards and Technology (NIST), and which are listed in the box below. Some agencies are clearly at Level 3, but the enterprise as a whole is at a Level 2 rating. For States using NIST Metrics, all strive to achieve Level 5, a fully integrated comprehensive information security program

NIST Metrics				
Level 1 Control objective documented in a security policy	Level 2 Security controls documented as procedures  Current Level of State as a Whole	Level 3 Procedures have been implemented	Level 4 Procedures and security controls are tested and reviewed	Level 5 Procedures and security controls are fully integrated into a comprehensive program

The Auditor General has recognized the need for a greater focus on security and privacy issues at a statewide level. The Auditor General recognizes the increasing risks and vulnerabilities associated with operating critical systems. The 2005 Auditor General report of GITA (05-03) identified strategic and organization gaps for the statewide management of information security.

In preparation for assessing more detailed system level risks, the Auditor General has recently added five new auditors primarily focused on IT systems audits. However, the commensurate governance and

investment in security planning and oversight at the State level has not yet been made. As a result, it is likely that ongoing security program gaps will be identified by the Auditor General for systems that fail to adequately protect critical State operations or citizen privacy. However, the five auditors will only be able to review a limited number of systems each year and may only be able to review specific systems on a periodic basis. In the meantime, the State will be accepting significant risks to data unless an effective information security governance program can be established to continuously identify risks and drive justified risk mitigation efforts.

Information security has become an essential business function, critical to enabling agencies to conduct operations and deliver services to the public.

The proposed SISPO and the IT auditors with the Auditor General's Office will complement one another to cover the level of risk identification/control (SISPO) and audit (Auditor General) needed by the State for these critical business functions.

3. INFORMATION RISK OVERVIEW

The State of Arizona faces many of the same risks that any other public or private organization expects to encounter. The risks include: 1) breach in data confidentiality, 2) loss of data integrity and 3) disruption of mission critical services. The source of those risks is summarized in the following table:

Human	Non-Human
Terrorist <ul style="list-style-type: none"> • Cyber Terror • Physical Terror • Blackmail 	Acts of Nature <ul style="list-style-type: none"> • Flood, Earthquake other weather-related threat • Disease Outbreak • Pandemic • Fire
Hacker <ul style="list-style-type: none"> • Disruption of Operations • Theft (IP, Assets, Identity) • Corporate espionage 	Environmental Disaster <ul style="list-style-type: none"> • Toxic Contamination • Anthrax Attack
Employee <ul style="list-style-type: none"> • Willful Misconduct or Revenge <ul style="list-style-type: none"> ▪ Former Staff (including terminated employees) ▪ Current Staff (curiosity, revenge, monetary gain) • Inadvertent or Accidental Misuse <ul style="list-style-type: none"> ▪ Accidental impact (Human error or poor training) ▪ Poor system configuration ▪ Unaware of threats and remediation • Negligence • Lack of Oversight for Security Program and Enforcement of Policies 	Interruption of Utilities <ul style="list-style-type: none"> • Electrical • Water • Telecommunications • Heat or Cooling
Contractor or Service Provider Abuse <ul style="list-style-type: none"> • Willful misconduct or theft • Poor vendor security controls may allow staff to misuse privileges • Inadequate vendor controls and monitoring 	Regulatory Compliance <ul style="list-style-type: none"> • Federal Regulations: HIPAA, GLBA, FISMA, Justice • NERC and associated Utility Security Standards to protect system availability
Competitor and Third Parties <ul style="list-style-type: none"> • Remote access (electronic theft, business intelligence gathering or fraud) • Local (theft of computing assets or electronic information) • Stolen laptops and information stored on laptops 	Technology Obsolescence <ul style="list-style-type: none"> • Improperly configured systems • Inability to reduce vulnerabilities through system management • Inability to recovery outdated platforms or the data stored on unsupported systems

Essentially, Arizona faces many potential risks and the actualization of those risks could have severe consequences. To determine the level of risk, the State must consider impact in the following likely areas

- **More frequent service disruption:** The Computer Security Institute / FBI 2006 Cyber Security Report identifies that virus attacks are the most prevalent risk experienced by security officers interviewed this year. The testing by CSI / FBI of anti-virus systems in

2006 resulted in none of the organizations tested passing that part of the assessment.⁹ Accordingly, service disruptions due to virus attack or other more directed attacks are to be expected. In one state, the W32 spybot attack in early December 2006 caused a significant outage on several mission critical systems. Several agencies of that State experienced an impact from an access through a single attack vector since the agencies' systems were connected.

- **Lessened homeland security:** Cyber Security has been identified by the FBI as an area of significant risk to critical infrastructures used to provide mission critical government services. Unauthorized access to mission critical systems by terrorists could disrupt the operation of government and service to its citizens. In addition to hacking into State systems, terrorists could—in some cases—be hired on as government employees by using false identification. The most recent raids of the Swift meat processing facilities in both northern Colorado and Texas underscore the ease with which fraudulent identification documents are obtained and used to obtain employment.
- **Escalating financial and legal liability:** While the state has enacted limitation of liability legislation for many risks, cyber risks introduce new types of financial and legal liability. The liability ranges from fines and penalties imposed by industries like the Payment Card Industry to the cost of providing notice to those citizens whose data has been compromised. In most cyber incidents, the resulting remediation program is also unbudgeted and disruptively focuses government IT departments on costly programs like that which the VA had to implement to prevent future loss of data from laptop computers. Citizens are demanding increased protection, which results in escalating liability.
- **Erosion of citizen trust in government:** As increased service disruption occurs due to cyber related vulnerabilities and threats, citizens turn to their government for accountability. These threats can occur from many sources with current attention being paid by the Federal Government to the homeland security terrorist threat. As a result of increased activity and awareness, there is a surge of current and pending legislation that increases regulatory requirements on both commercial and governmental interests.

Historically, the public accepted the fact that cyber threats were quickly emerging and that existing controls might not be adequate. However, increased awareness of identity theft and the realization that sophisticated criminal and terrorist organizations may be behind some cyber-threats has increased citizen expectations for security. All these factors cumulate in States need for tighter control and more oversight to avoid the danger of eroding or undermining citizens' trust in their government.

“Arizonans have been adversely impacted by identity theft. To be effective, the new office must be proactive on issues concerning citizens’ privacy.”

**—Joe Throckmorton, CIO
Arizona Department of Transportation**

⁹ CSF/FBI 2006 Computer Crime and Security Survey

To summarize, "Our data shows that, in spite of the increased attention being paid to the issue of data security, enormous gaps remain in the ability to effectively protect sensitive data, and that a lack of accountability as well as a dearth of resources dedicated to the problem are at the root of the problem," observed Dr. Larry Ponemon, chairman and founder of the Ponemon Institute. "As we have shown in the past, the costs associated with a data breach can be steep, yet many companies have been slow to address this issue in a meaningful way. Based on our findings, we believe that establishing clear accountability, as well as investing in training and technology can help organizations best leverage their existing resources, close these gaps, and better protect information assets, including customer data and intellectual property."¹⁰

¹⁰ August 28, 2006 Press Release from Poenemon Institute

4. WHY SISPO IS A BEST PRACTICE

A best practice is a technique, process, or methodology that, experts agree is appropriate, accepted and widely used, and has proven to reliably lead to a desired result.

When examining the state of information security over a broad spectrum, there are some baseline trends that emerge as best practices. There are several leading information security organizations that recommend organizational best practices and they all advocate common core requirements.

In the *Global State of Information Security* study, the organizations deploying best practices more frequently had senior security or privacy positions (CISO or CPO) in their company than the survey base. Best practice organizations have clearly adopted long-term, risk-based security strategies more so than their counterparts. The greatest barriers to good security—limited budget, limited staff—were common to the best practice group as well as the overall survey respondents. However, time invested in mitigating security risks was greater for the best practice group

The Information Systems Security Association (ISSA) utilizes Generally Accepted Information Security Principles (GAISP), which are a consensus as to the principles, standards, conventions and mechanisms that information security practitioners should employ, that information processing products should provide, and that information owners and organizational governance should acknowledge. The goal of GAISP is to ensure the security of information and the information systems that house such information.¹¹

Oversight and monitoring of agencies was a key approach to GAISP's best practice of affixing appropriate responsibility to the owners and providers of information systems. Inclusion of executive management in the development of a clearly articulated hierarchy of IT security policies is also a GAISP best practice.

The International Standard Organization (ISO) has developed its ISO/IEC 17799 standard to specify a management framework that controls and assigns clear responsibilities for policy development to an organization, which can then reach across the organization to institute change and ensure compliance.¹²

Information security and privacy government leaders in other states were interviewed to identify best practices they use in developing their information security programs. The State of Arizona's proposed SISPO conforms to the viewpoints of industry and governmental leaders regarding the roles and responsibilities of such an office and what is required for successful information security governance. The SISPO is recommended to embrace the functions of like organizations in other states as well as establishing a CISO and CPO to provide the leadership for these functions.

“...it is critical that CISOs and CPOs have a place at the Executive management's table. More and more state governments are adopting the private sector model by establishing CISOs and CPOs positions at the highest levels.”

**- Will Pelgrin
Director
Cyber Security and Critical
Infrastructure Coordination,
New York State and Chair of the
Multi-State Information Sharing and
Analysis Center.**

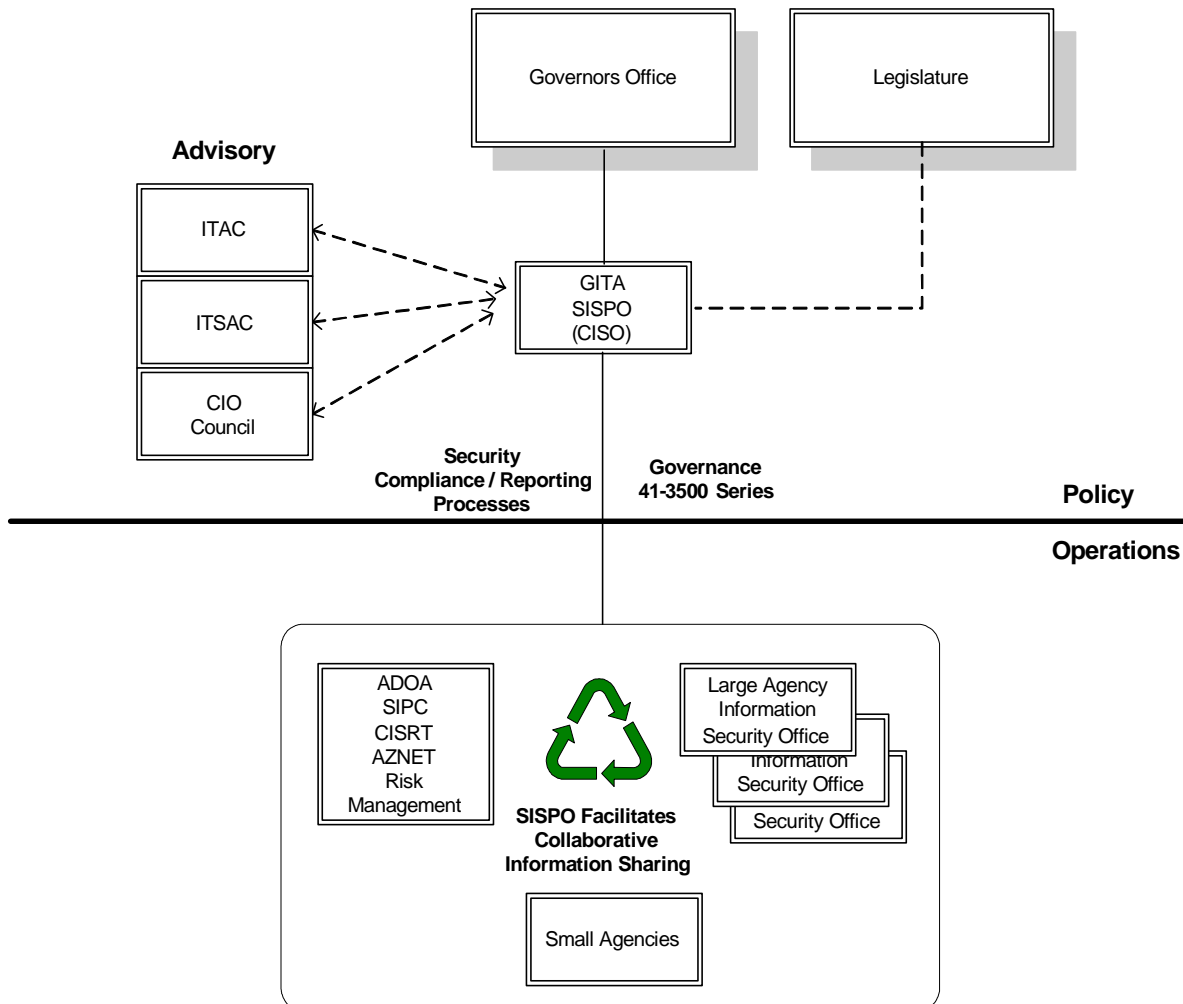
¹¹ Generally Accepted Information Security Principles, V3.0, 2004 Information Systems Security Association

¹² ISO/IEC 17799, International Standard, Code of Practice for Information Security Management.

5. SISPO COMPONENTS AND RESPONSIBILITIES

As an oversight function, the primary responsibility of the SISPO is to enhance the protection of State information resources and citizen privacy by maintaining statewide information security and privacy policies and leading the implementation of statewide security planning and policy enforcement to mitigate risks. Since the State currently operates information systems in a decentralized manner, each agency has been responsible for its own security programs. Some agencies are already deploying effective controls but those controls are not consistently deployed or effectively monitored to ensure the entire system of state operations is protected. Just as important, the ongoing effectiveness of those controls is not measured or reported to the chief executive of the State. The goal of the SISPO is to “federate” the decentralized operations into a uniform deployment of baseline security and privacy standards to provide “reasonable” protection for all information resources.

The SISPO responsibilities would integrate well with the operational security functions performed by AZNet for shared Information Technology (IT) services and the security operations of individual agencies. The SISPO should not manage any security operations or replace any security operations already in place at agencies.



The governance model recommended as the security best practice for Arizona complies with guidelines published by NIST.

SISPO Responsibilities

Security & Privacy Program Development

The cornerstone of SISPO's responsibility is integrated statewide program development. Privacy policy dictates ***how a state will collect and use citizen's personal information and data***. Security policy dictates ***how a state will protect that information from misuse or loss***.

By creating and enforcing a common set of standards that have been developed to mitigate known risks to State information resources, the agencies can develop and deploy security and privacy programs with the confidence that their programs will meet baseline requirements clearly defined by State experts. Without a common understanding of critical program elements, statewide integration of systems and information sharing will be subject to the lowest standard set by any single agency. By clearly communicating baseline standards, the SISPO can drive the state toward cost effective enterprise level security solutions in a federated model that supports agency level risk mitigation for decentralized operations.

“I feel it is important to organize around what the chief information office is authorized to do by law, empowered to do by the governor, and encouraged to do by the agencies.”

- Mary Carroll, CIO
Ohio

Security Standards Oversight

The effectiveness of the statewide security program will depend upon the amount of oversight provided. If no one is “minding the store,” the standards will not be continuously deployed or operate effectively. Therefore, the SISPO should have responsibility to manage a program for the agencies to measure and periodically report effectiveness of the controls deployed within their agency. This oversight will not only serve to enforce current baseline standards but also provide input into the security planning process. If current standards are not routinely achieved, the SISPO can consider program adjustments based upon feedback from the oversight process.

Compliance Management

The SISPO would establish a compliance office to manage continuous compliance with Federal and State Information and Privacy laws. Since 2000, over a dozen new information security laws that include the protection of health information (HIPAA), consumer financial information (GLBA) and a wide range of personal privacy regulations have been enacted. The compliance management office should consolidate a list of compliance requirements throughout the State and track compliance status for each requirement. The SISPO office will provide periodic compliance status reports to State leadership.

Security Analysis and Support

The SISPO should maintain the expertise to understand risks to State information resources and develop control standards to mitigate those risks. The Security analysis function will directly support the SISPO in the development of security standards and will also be available to the agencies to guide the selection, acquisition and deployment of specific controls.

This shared “expert” set of resources would respond to security questions and facilitate support to both the SISPO and the agencies to solve security problems. Initially, the security analysts will support the SISPO and agencies supporting the development of agency level security plans. While each analyst will have specific skills, the intent is to maintain a senior level analyst who can support security planning and governance as well as more junior analysts who can assist in the design of controls and evaluation of alternatives. Additionally, the staff assigned to security analysis and support may help respond to a cyber incident.

“Small agencies create potentially the most vulnerability for Arizona’s information network because they do not have coordinated security and privacy programs.”

**- Ron Hardin, CIO
Arizona Department of
Environmental Quality**

Incident Response

The SISPO would have the responsibility and authority for incident response oversight within the executive branch. The ability to provide oversight of incident response is directly linked to the resources available based on the phased deployment of the office.

The SISPO should develop the capability to analyze, report and respond to the actual or suspected loss or unauthorized access to personally identifiable and sensitive State information. This function develops the incident response program and provides oversight on any major response during a statewide cyber incident. The SISPO should plan and coordinate, in partnership with AZNet and ADOA to develop and deploy a statewide event management and incident response capability. The SISPO should have the authority for statewide and interagency coordination as well as the ability to direct responsibility for incident response. However, ADOA and agencies with dedicated network staff are expected to continue providing operational support that will include agency system monitoring, event tracking, incident containment and system recovery.

The SISPO would also provide (as qualified resources are added to the SISPO in later phases of office deployment) the coordination required for forensic information gathering, threat monitoring, law enforcement liaison, central incident reporting, analysis and sharing of lessons learned.

Training & Awareness

The SISPO would develop a security training and awareness program to assist in the delivery of security and privacy training throughout the State. Training agency personnel in effective security and privacy best practices is one of the most important functions of the SISPO. The goal is to provide a central facility for all agencies to educate staff, contractors and potentially citizens on the threats to information resources and risk mitigation strategies to protect citizen privacy and sensitive State information resources.

SISPO Organization

To fulfill the responsibilities listed above in the most efficient manner, we recommend that the SISPO be deployed in a phased approach over three years with staff added each year.

Phase/Year	I – Focus on Risk Identification & Agency Education	3 FTE
Phase/Year	II – Focus on Security Program Implementation	8 FTE
Phase/Year	III – Focus on Metrics and Program Adjustment	<u>2 FTE</u>
		Total 13 FTE

After reviewing State requirements and best practices deployed in other states, we believe that GITA provides the most efficient structure to deploy the new SISPO organization.

By deploying the SISPO within GITA, the new security organization can leverage:

- Current authority to publish and maintain security standards via a proven change control process,
- Relationships and communications structure to facilitate comprehensive risk assessment and security planning, and process,
- The information technology enterprise knowledge base to assist in the coordinate and support activities Relationships

Phased Implementation

A summary of the phased implementation is outlined in the attached table. As resources are allocated to the SISPO over a three year period, the SISPO will “stand up” functional components identified in each of the phases.

Phase/Year	Functional Components	Resources	Key Staff Required
I	<ul style="list-style-type: none"> Security & Privacy Program Development Conduct Statewide Risk Assessment Training and Awareness 	<ul style="list-style-type: none"> ◆ ✓ ◆ 	<ul style="list-style-type: none"> CISO CPO Security Training and Awareness Specialist
II	<ul style="list-style-type: none"> Security & Privacy Program Development Security Standards Oversight Compliance Management Security Analysis and Support Incident Response Oversight Training and Awareness 	<ul style="list-style-type: none"> ✓ ✓ ✓ ◆ ◆ ✓ 	<p>Staff include all key personnel from phase I plus the following staff:</p> <ul style="list-style-type: none"> 2 Security Analysts (1 Senior & 1 Mid-level) 1 Compliance Manager 2 Threat & Vulnerability analyst 1 Incident Response Coordinator 1 Assessment specialist 1 Forensic specialist
III	<ul style="list-style-type: none"> Security & Privacy Program Development Security Standards Oversight Compliance Management Security Analysis and Support Incident Response Oversight Training and Awareness 	<ul style="list-style-type: none"> ✓ ✓ ✓ ✓ ✓ ✓ 	<p>Staff include all key personnel from phase I and II plus the following staff:</p> <ul style="list-style-type: none"> 2 Security Analysts (Mid-level)

✓ = Resources designated for this phase are adequate to accomplish the function

◆ = Resources designated for this phase are adequate to start planning

Bottom Line

In order to have a successful statewide information security program, the State must recruit, train and effectively manage skilled and experienced security professionals in a central organization that has both the authority and resources to perform assigned responsibilities. The phased implementation listed above provides for the baseline governance and oversight functions needed for an information security program. While the resources required to implement the program in subsequent phases are based upon industry best practices, this estimate may change to some degree after the risk assessment in Phase I quantifies the level of risk and detailed requirements for risk mitigation.

6. INDEPENDENT RISK ASSESSMENT

Why a risk assessment?

By accomplishing an inventory of risk on its information technology systems and assets, the State can prioritize protection for the most “at-risk” systems. This will allow management to rank the order of remediation plans and efforts and align these efforts to available resources. By base lining with a statewide risk assessment to capture the scope and breadth of the problem, the State employs the first step in reducing its overall risk in the most effective and efficient manner. The most at-risk systems and highest liability assets holding the most critical data will then be categorized and (once resources are identified to remedy these risks) the overall risk to the State will be lowered in the most expeditious manner.

Many organizations use both self-assessments and independent audits to provide for a balanced risk analysis of their organization. Self-assessments of information security occupy an important role in preparing the organization for a formal review. The formal review or independent risk assessment is needed for an organization’s management as it removes inherent internal bias and protectionism. Human nature compels one to defend his or her own work, and so self-assessments require additional controls to be judged valid by outside parties. Compliance auditors generally view independence more favorably.

In the CSI/FBI 2006 Computer Crime and Security Survey 62% of the respondents used security audits by an external organization.¹³

There are several important reasons to have an outside independent risk assessment.

- The independent risk assessment can provide externally validated status and an indication of security vulnerability and risk.
- In most cases, there are internal information technology experts that are systems users and administrators on the systems that are being run. However, due to the specialized nature of information technology it is usually difficult to find the skill sets necessary to accomplish a top down risk assessment from within an organization that has sufficient breath and depth to uncover the existence of all vulnerabilities. It is a best practice and procedure to run self-assessments only in preparation for independent assessments.
- It is important that the independence of the assessor be maintained and is not comprised by vendor relationships that may be at cross-purposes to obtaining a true picture of the risk. An independent assessor when asked, based on their experience, what type of software or hardware solution should be used does not have a profit motive behind their recommendation.
- An independent third party assessor will not be drawn into day-to-day operational activities that inevitably happen to the employees of the enterprise conducting a self-assessment. There is a project plan with a start date and an end date with precise deliverables and a higher likelihood of project completion.

¹³ Ibid.

The following chart lists some of the pros and cons to conducting the assessment in house versus outsourcing:

	Pro	Con
Internal Assessment (In House)	<ul style="list-style-type: none"> - Closer to risks - Can drive controls - Knows the environment 	<ul style="list-style-type: none"> - Possible lack of expertise / skill sets - Too close to problems - High risk project may not be completed on a timely basis due to operations distractions
Independent Third-Party Assessment (Out Source)	<ul style="list-style-type: none"> - Specialized expertise in assessments - Input from another organization (baseline / fresh perspective) - More independent & objective - Less distracted by operations - More likely project will be completed in a timely basis 	<ul style="list-style-type: none"> - Costs more - Still requires knowledgeable agency input - Lack of specific background re: the environment

Cost of Independent Assessment

The State of Arizona would be best served by conducting a complete risk assessment for all agencies, boards and commissions. The implementation of the risk assessment should be based on a best practices approach such as the NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems. This type of approach first identifies the mission critical systems and data that are most important to the functioning of the State. Using this identification a third party risk assessment contractor would be tasked to identify overall information security risk during a detailed risk assessment of the most valuable information assets and the resulting remediation required.

Our experience has shown that the larger agencies require a more in-depth assessment of the systems than the smaller agencies but also have the majority of the mission critical systems. The costs vary between agency types and sizes but we have found they generally fall in the range of \$5,000 to \$50,000. For comparison, the State of Florida conducted a critical infrastructure assessment about three years ago that was estimated at \$2.0 million. Coalfire is estimating an average cost to conduct a risk assessment of approximately \$15,000 for each of your agencies.

The resulting total of \$1.5 million is budgeted to complete this critical first step in statewide information security.

Based on identified vulnerabilities, threat mitigation strategies will need to be deployed immediately with appropriate follow-on compliance testing. Mitigation costs vary based on the vulnerability, magnitude of

threat, and the value of the asset being protected and will be determined based on the results of the statewide, independent risk assessment.

Recommendation

We recommend the best practices method for conducting enterprise risk assessments using independent third parties to perform the assessment. This provides the opportunity to have an independent third party conduct the baseline assessment under the direct supervision of the SISPO along with direct input from the agencies. After the conclusion of the independent assessments, appropriate internal self-assessments should be conducted on a regular basis. Periodic independent third party assessments and/or internal state audits on a programmed multi-year basis, normally every three to four years, would continually validate the overall statewide compliance program.

7. SUMMARY of SISPO FUNCTIONS

As summarized in section 5, the six (6) primary functions identified for the SISPO to be successful include:

- a. Security and Privacy Program Development
- b. Security Standards Oversight
- c. Compliance Management
- d. Security Analysis and Support
- e. Incident Response
- f. Security Training and Awareness

7a. Security and Privacy Program Development

Description of Function

The Security and Privacy Program Development function should establish the framework for both statewide security and privacy programs. The SISPO will coordinate security planning throughout the State as well as establish a baseline of security controls to protect the privacy of citizen data and other critical State information assets that enable secure and reliable delivery of services.

One of the primary goals of the SISPO should be to create a governance program that leads the different agencies and budget units to adequate information security within their organizations. The SISPO formalizes a State Chief Information Security Officer (CISO) and Chief Privacy Officer (CPO) role within the State to provide the leadership to federate controls and establish enforceable information security and privacy policies and standards.

Unlike AZNet and ADOA, the SISPO will not perform operational functions. The SISPO will be a policy development and information security governance office. Agencies will continue to operate systems and protect data in a decentralized environment.

“It is important that SISPO provide strong governance and leadership in the areas of privacy and security.”

**- Patrick Quain, CIO
Arizona Department of
Administration**

Rationale and Justification for the Function

Service delivery within Arizona state government is evolving as follows:

- The reliance on information technology to deliver State services continues to increase.
- The push towards E-government platforms to accelerate service delivery as well as reduce the costs of service delivery continues.
- The pervasiveness of information sharing within the State and with 3rd parties who support the State exposes sensitive data to greater potential compromise.
- The decreased tolerance of citizens to government failures to protect their privacy increases the State's need to provide greater protection.

The combination of these factors is driving the State to establish and maintain the SISPO. The program development function is necessary to integrate the SISPO functions with one another and with existing programs to address evolving requirements.

Key Activities for this Function

In order to have an integrated statewide information security and privacy program that has the responsibility, necessary authority and resources to protect the State's valuable information assets there must be a strategic plan and the ability to effectively communicate the plan to all stakeholders. Critical elements of the planning process include:

- **Vision**

The key SISPO staff should have the expertise and credibility to understand the State environment and to communicate the strategy for protecting State information resources and citizen privacy. The CISO and CPO will advise State leadership on security and privacy matters, establish a clear vision and consistent message for the State's security and privacy activities, and coordinate programs to achieve security and privacy objectives.

- **Leadership**

The CISO and CPO should provide the leadership to effectively deploy and enforce the security and privacy programs. The success and failure of other state and federal security programs around the country has been tied to the effectiveness of these individuals as much as to the policies and standards in place for each security program. **The State should conduct a national search to confirm that these key leadership roles are filled by the most qualified candidates possible.**

- **Risk Assessment**

To validate and justify the standards, the SISPO should manage a statewide information risk assessment and maintain a current understanding of the risks that threaten State information resources. The risk management function will enable an identification of the criticality rating for each system and will provide a review of current threats and potential impacts from those threats to guide selection of controls and associated standards.

- **Creation of Policies and Standards** - The security and privacy program will include the creation and update of existing privacy and security policies and standards. Development of stronger IT security standards will involve consensus building and discussion since agencies currently have varying systems, architectures and are at different stages in their system and security protection lifecycles.

“As the CISO in Michigan over the past 4+ years, I can tell you that this is not an exact science. Every state does things a bit differently and has different models for centralization of IT and their security functions.

**- Dan Lorman
Chief Information Security
Officer, Michigan**

Security policies dictate how a State will protect information from misuse by those internally as well as externally.¹⁴ Security is how privacy is protected and the measures that an organization takes, including virus protection, firewalls, roles-based access to sensitive information and intrusion detection systems, to ensure that personal information is not accessed or used in a manner that is contrary to privacy policies. Arizona has recently taken steps to address information security through the enactment of a security breach notification statute.¹⁵

Privacy policies dictate when and how a State will collect, store, use, disseminate and dispose of sensitive personal information of its citizens. Privacy is a personal construct that accrues to individuals, not to the information itself. In other words, a person has the right to have certain personal information kept private by the State and accessible only to those state employees who need to use the information in their duties.

Resource Requirements

The program development function will require a staff of two Full Time Equivalent (FTE) staff members. These FTEs include:

- Chief Information Security Officer (CISO)
- Chief Privacy Officer (CPO)

The program development function requires a combination of technical expertise and leadership ability to effectively integrate statewide security and privacy programs into existing State operations. The skills required to effectively perform these roles at an enterprise level are in very high demand nationally due to the recent wave of security and privacy regulations. The recruiting and budget process will have to be tailored to attract and retain the “right” leadership for the SISPO.

The function will require an office that can be segregated to protect sensitive security and privacy planning information and will incur overhead expenses for space, computers, systems, subscriptions, conferences, etc. The Chief Privacy and Security Officers will be internal facing to lead program deployment as well as external facing to participate in nationwide security and privacy planning functions. The office has accordingly requested \$295,300 in the first year for three staff (includes a training/awareness specialist (see training function below)) and office operations.

The comprehensive risk assessment (\$1.5 million) will be required (see section “Independent Risk Assessment”) to enable the CISO and CPO to properly define the SISPO program and determine key risk areas for programming and mitigation. In addition, the office will likely require some future support from contractors for in-depth expertise on new threats or for consulting on critical incidents and challenges (cost will depend on challenges faced).

Critical Success Factors

Critical success factors for effective program development are listed.

¹⁴ NASCIO, Keeping Citizen Trust: What Can A State CIO Do To Protect Privacy?, October, 2006

¹⁵ State of Arizona Statue; 44-7501; Notification of breach of security system; enforcement; civil penalty; preemption; exceptions; definitions; 2006.

- The State must recruit the right leadership for the CISO and CPO positions.
- The SISPO and the agency security offices must be strong enough to perform assigned tasks.
- The State should implement an internal marketing program to ensure all stakeholders understand the authority delegated to the SISPO.
- The SISPO should establish a cooperative working environment with the agencies to ensure the security planning process is responsive, collaborative and effective.
- The State should allocate adequate funding to complete a comprehensive risk assessment to establish a baseline against which to establish controls.

7b. Security Standards Oversight

Description of Function

Security standards oversight includes the establishment of consistent metrics to measure the operating effectiveness for each control and the routine reporting to evaluate the progress of agencies to meet baseline security and privacy policies and standards. The oversight function also includes reporting to both State Executive Management and the Legislature to provide transparency of risk mitigation efforts within the State.

The standards oversight function will leverage the comprehensive risk assessment to enable the refinement and alignment of proper standards and controls. The staff supporting this function will then encourage factual reporting to identify barriers to effective deployment of the control or standard.

As many of the larger agencies within the State have identified, the entire State is at risk when the baseline security controls are not uniformly deployed. The Standards oversight function will collect the data necessary to validate uniform deployment of baseline controls and will recommend changes to the controls or standards from time to time based on evolving threats and operating environments. This staff will also review annual IT security plans from each agency to track progress in mitigating known risks.

"In dealing with other agencies that you are connected to it's all about trusting their network and this occurs by knowing they are following the agreed upon security standards. "

**- Doug Robinson
Director, NASCIO**

The office is the representative for the executive branch concerning information technology homeland security matters and requires the authority necessary for enforcement of security policies and standards to address those threats.

Rationale and Justification for the Function

By strengthening common State security and privacy standards, agencies will have a defined framework to enable coordinated security planning.

By establishing well defined metrics, reviewing annual IT security plans for gap closure plans and measuring control objectives to defined standards, those who have fiduciary duty to protect critical information resources and citizen privacy will have a yardstick to demonstrate performance to that fiduciary duty.

The standards oversight function will provide the transparency to both the standards deployed to protect State information resources as well as the compliance with those controls and standards by State agencies.

Key Activities for this Function

The key activities for the SISPO in security and privacy oversight are summarized below.

- Strengthen existing uniform and justified baseline security and privacy standards and guidelines for the protection of State information resources and citizen privacy.
- Develop IT security plans and metrics to measure the effectiveness of controls specified in the security and privacy standards.
- Develop a self-assessment methodology and require each agency to submit annual self-assessments to the security and privacy standards.
- Each agency will prepare an annual information security plan and submit it to the CISO. The CISO will compare security plans to the known risk to State information resources and the baseline controls defined in State policies and standards. Any gaps in protection for citizen privacy and sensitive State information will be identified and the CISO will coordinate with agency executives to close gaps.
- Review agency self-assessment reports. Provide feedback to the agency with recommendations to improve controls or accelerate high priority controls within the agency Plan of Action and Milestones submitted with annual security plans.
- Collaborate and coordinate with other budget units to ensure standards are achievable and aligned with state business needs.
- Provide routine reporting of control effectiveness to State executives and the legislature.
- Oversight of the State acquisition and development processes to assure State information security and privacy standards are integrated into new or significantly upgraded systems.
- Maintain oversight of privacy protections through evaluation of agency exception reports and citizen complaints.

Enforcement

The key enforcement processes for information security and privacy standards recommended are:

- Each year, the agencies must submit an information security plan to the SISPO for approval. If the plan is not approved, the SISPO has the authority deny accreditation for the system to operate without program adjustments. This lack of accreditation will require the agencies to submit a revised plan to demonstrate that baseline security standards will be implemented within an acceptable period.
- During the budget process, all new systems or major upgrades to existing systems require approved Project Investment Justifications (PIJs). These PIJs will be reviewed by the CISO

as well as other GITA staff. The SISPO will thereby have input before project approval and ensure compliance with the statewide baseline security standards for new or significantly upgraded systems.

Resource Requirements

The standards oversight function will be provided by the Security Analysis and Support team - 4 staff (2 in Year 2; 2 in Year 3). This team will also support provide another function (Security Analysis and Support, see below). The Senior Security Analyst will support the CISO in upgrade and updates of security standards and review of routine agency reporting of control deployment to those standards. The CPO will develop privacy standards and will maintain oversight through evaluation of both agency exception reports and citizen complaints.

Critical Success Factors

Critical success factors for the security oversight function include:

- Establishing measurable controls in each of the security and privacy standards.
- Effective oversight of the standards to ensure uniform implementation.
- Obtaining concurrence and support from the legislature and State Executives to provide the resources that enable State agencies to comply with the standards.
- Ability to effectively enforce the standards through the PIJ and plan oversight processes.

7c. Compliance Management

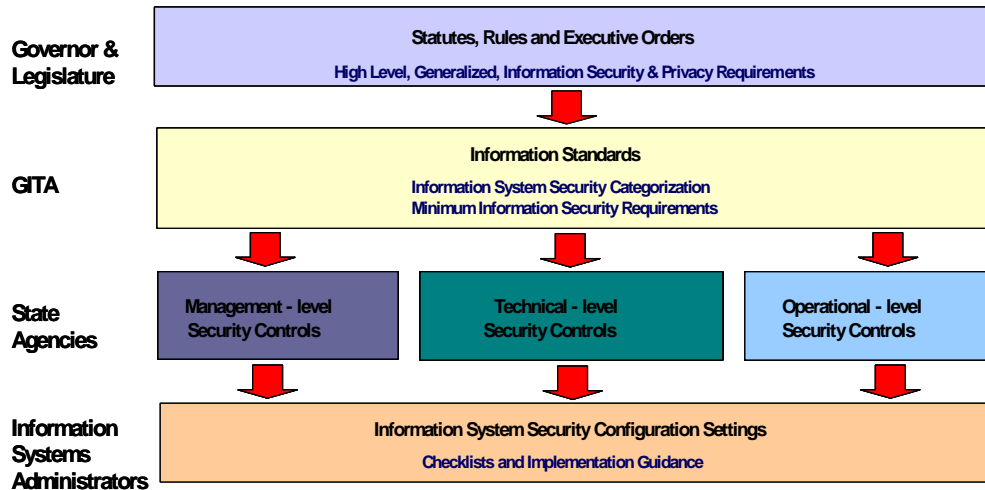
Description of Function

The SISPO would create a compliance office and will designate an information security and privacy compliance officer to manage compliance to State and Federal laws. The primary functions of the compliance office will include:

- Inventory State data and systems
- Consolidate a list of security and privacy compliance requirements (i.e., HIPPA) impacting all areas of State government
- Advise agencies on compliance requirements
- Track compliance status of agencies
- Report compliance status to State Executives and the Legislature.

The compliance model (in the adjacent diagram) outlines the compliance lifecycle from legislation to compliance management. While the State has deployed some compliance programs within

Compliance Model



agencies, this new statewide compliance function will establish oversight and governance to help improve compliance. The compliance office will work closely with the security standards oversight team and the Auditor General.

Rationale and Justification for the Function

The State of Arizona has enacted liability containment legislation to protect the State against a wide range of claims for information security breaches. However, since compliance requirements for information security and privacy are defined in federal and state statutes, the failure to implement compliance management oversight will leave the State open to claims of negligence. Implementation of compliance management will demonstrate that reasonable controls have been deployed and are being monitored. Failure to demonstrate effective compliance management may lead to increased liability during future data breach incidents.

Key Activities for this Function

The SISPO would perform the following key compliance management activities;

- Analyze federal and State information security and privacy regulations and maintain a summary of laws that require compliance oversight by the State.
- Establish “change management” protocols to track changes in the laws or to individual areas of regulation and to notify agencies about these changes.
- Utilize inventory of State systems and data to assist agencies in determining the level of security compliance required for each subject area of its operations.
- Coordinate with the Auditor General to conduct independent testing to established compliance

“We have the authority to shut down offending agencies if enforcement is required.”

**- Mark Weatherford
CISO State of Colorado**

requirements, if required by laws or justified by risk.

- Establish a program to enforce information security and privacy compliance by 3rd parties and service providers. Maintain records of vendor and service provider compliance.
- Develop an agency annual report of compliance with state and federal regulations and review these reports when submitted.
- When justified, attend seminars and subscribe to publications and updating services to stay current with key compliance requirements and regulations

Resource Requirements

This function would require a full time compliance manager. The compliance manager will require a subscription to a compliance alert service and access to compliance experts.

An Assessment Specialist would provide capability to assess for some compliance activities.

This budget of 2 FTE plus access to compliance expertise is a reasonable starting point for this function.

Critical Success Factors

Critical success factors for the compliance management function include:

- Cooperation from agencies subject to compliance requirements.
- Independent testing to ensure compliance monitoring is adequately designed and operating effectively.
- Review of the acquisition and procurement plans of the agencies to determine if they are in compliance with state and federal security and privacy regulations.
- Certification of compliance to state and federal security and privacy regulations annually by senior management.
- **Enforcement** – Empowering the SISPO to implement sanctions to include the timely removal of unsafe systems from operations or to delay budget requests until adequate compliance monitoring is integrated into each appropriate system.

7d. Security Analysis and Support

Description of Function

The SISPO would hire and maintain security experts and analysts. The Security analysts will be available to the agencies to guide in the selection, acquisition and deployment of specific operational security and privacy controls meeting individual agency needs in keeping with statewide standards.

These “expert” resources will respond to security questions and provide support to both the SISPO and the agencies to solve security problems and lessen security risks. The security analysts will support the SISPO and agencies in conducting risk assessments and completing agency level security plans.

While each analyst should have specific skills determined to be helpful by the initial baseline assessment, it is also common to maintain a senior level analyst as well as some junior analysts who can assist in the design of controls and evaluation of alternatives. The staff

assigned to security analysis and support could also be deployed to also support incident management staff when warranted by the criticality or extent of incidents.

Rationale and Justification for the Function

Without the security analysts, the SISPO will become a figurehead function lacking the critical resources or expertise to truly add value to agency security operations. The security analysts are the staff that will work with the 110 agencies on operational implementation, self-assessments, agency level plans, etc. in support of improved security and privacy protection statewide.

The Gartner Group asserts that over 90% of attacks exploit known vulnerabilities.¹⁶ While the vulnerability analyst in the Incident Response office will track vulnerabilities and provide warnings and alerts. The security analysts will be dispatched to agencies to help with remediation advice and provide best practice guidance to prevent future vulnerabilities.

Key Activities for this Function

The tasks and skills necessary to fulfill this function are:

- Hiring of experienced security analysts who have:
 - Operational experience but who can now guide agencies rather than simply operate systems.
 - Extensive security control expertise on systems with similar characteristics to the agencies they will support.
 - Ability to perform security research and analysis on multiple systems for disparate agencies.
 - Ability to provide threat and alert remediation support
- Incident recognition processes in place to activate when necessary to escalate to incident response.

Resource Requirements

The security analysis and support function will require one senior security analyst and three mid-level analysts to perform security standards oversight (see above) as well as security analysis and support, including conducting research, reviewing security processes and products and providing “expert” advice to the SISPO and the agencies.

Critical Success Factors

Critical success factors for the security analysis and support function include:

- Availability of the security experts to agencies for knowledge transfer.
- Keeping the analysts’ knowledge current regarding new vulnerabilities and threats.
- Establish continuous monitoring of the health of the state information systems.

¹⁶ <http://www.infosecurityproductsguide.com/whitepapers/6206510009.html>

7e. Incident Response

Description of Function

Incident response involves detecting, reporting and responding to actual or suspected loss or unauthorized access to personally identifiable and sensitive state information.

The CISO would be the Chief Incident Manager to whom all incidents impacting State government are reported. Agencies will be required to report cyber incidents to the SISPO.

The SISPO would design an incident response program, guide the response during cyber incident with major impact and maintain cross agency authority for incident response. The SISPO should coordinate with AZNet and ADOA to develop and deploy a statewide event management and incident response system/facility. ADOA and agencies should continue to be expected to provide operational support that will include system monitoring, event tracking, incident containment and system recovery.

The SISPO should provide the coordination required for forensic information gathering and interfacing with law enforcement personnel. The SISPO should also monitor alerts and warnings for potential attacks and publish guidance about threat warnings. The agencies should document the event. The SISPO should maintain a repository of such documentation, identify lessons learned and lead the post incident brief after recovery from the incident.

“Statewide capabilities to respond to critical incidents must be enhanced before a major security breach with significant consequences occurs.”

**- Jim Ryan
Homeland Security Technology
Manager, GITA**

Rationale and Justification for the Function

Cyber incidents occur daily and firewall engineers understand that firewalls are attacked many times every hour. If only one of these cyber attacks compromises a single system, serious consequences can result (i.e., compromise of citizens personal information, compromise of sensitive emergency response planning information, destruction of critical State information, etc.). Accordingly, the State must deploy an effective incident response capability to rapidly identify, contain and recover from the impact of a successful cyber attack.

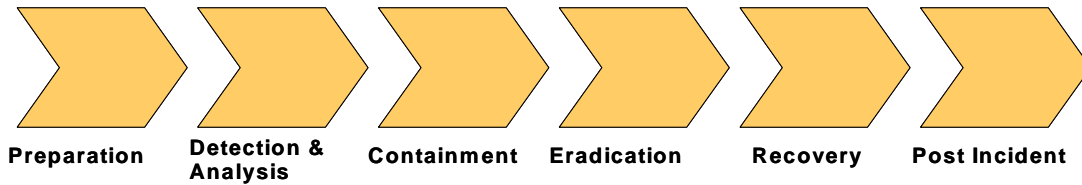
Beginning July 2003 with the enactment of California Bill 1386, the requirement for reporting the public about data breaches has been escalating. The civil and criminal sanctions for failure to notify consumers of data privacy breaches are significant.

In September 2006, the State of Arizona Notification of Data Breach law went into effect. The duty to notify consumers when data privacy is violated will likely cause a significant increase in incident reporting in the State. On January 25, 2006 MSNBC reported, “For the sixth year in a row, identity theft tops the annual list of consumer complaints collected by Federal Trade Commission.”

The incident response function will enable the State to respond to data breaches, to properly notify the public about such breaches when they occur and to respond to inquiries about breach notices from contractors, staff and 3rd party service providers.

Key Activities for this Function

The State must have the capability to detect, report, and respond to the loss or unauthorized access to personally identifiable and governmental information.



Incident Management Lead: The CISO or his staff designee would lead and/or coordinate with the incident response team for major events impacting Arizona state government. The SISPO will develop a policy that describes the types of incidents that will escalate to the SISPO for management and the kind that the agency will manage but that the SISPO will support and monitor.

The SISPO should conduct exercises to test its procedures for managing major incidents on a regular, statewide basis.

In other states, the fact that the SISPO can assume authority over an incident originating in a particular agency has resulted in agencies maintaining their incident response detection and response at a higher state of readiness. The generally accepted functions of information technology security incident handling revolve around six activities.

- **Preparation:** Incident response requires intensive planning to be successful. The team, whether it be standing or ad hoc, must plan, train and exercise in order to be effective. The incident response team should include some of an organization's most qualified information technology professionals.
- **Detection and Analysis:** With the wide variety of potential incidents, organizations cannot have specific procedures to handle every one. The most common approach is to prepare for the most common incidents and review after action reports from uncommon occurrences to glean lessons learned. Common precursors and indications are used to train personnel in incident identification. The analysis of indicators is not an exact science but there are many common practices to correct identification and analysis of an attack that staff should be well schooled in.
- **Containment:** Strategies to contain an incident depend on proper identification and analysis as well as the degree of impact. As a general matter, containing the spread of the impact of an attack is the highest priority for an enterprise, while eradication and recovery are in the works.
- **Eradication:** Once the incident is contained and its scope understood the focus can turn to eradicating or eliminating the problem. There are many solutions to eradications from applying patches and updating operating systems to replacing the hardware or software components by buying new systems.
- **Recovery:** Once the problem is eradicated the organization will need to recover from the impact of the event. Recovery can take days or weeks, depending on the preparedness for the incident and the extent of its impact.
- **Post-Incident Activities:** The key post-incident activities are development of an after action report, a lessons learned document, conducting an out-briefing of the persons

involved and distribution of after action and lesson learned documents to other areas of the organization (or other agencies) to enable them to learn from incidents handled by others. These activities tend to be overlooked which is very unfortunate because they are essential for prevention of an incident reoccurrence and for organizational preparedness for future incidents.

Resource Requirements

The Statewide incident response function requires:

- One full time Incident Coordinator to develop plans, train incident response stakeholders and provide support leadership during actual incidents.
- Two Threat and Vulnerability Analysts to monitor advisories, provide statewide alerts and to coordinate with other emergency response centers to coordinate response to regional or national incidents. The vulnerability analyst will also be responsible for periodic testing of critical State systems to identify vulnerabilities.
- One Forensic Specialist to investigate attacks on State systems.
- An information security test lab to support analysis and forensics.
- A training infrastructure that will provide dual functionality and address incident reporting systems needs.

It is anticipated that AZNet and/or ADOA will maintain the event monitoring, incident tracking and communications center to host the Incident Response Team during a cyber incident.

Critical Success Factors

Critical success factors for a statewide Arizona State government incident response function include:

- Plans and procedures for the hand off of an incident among agencies and between agencies and the SISPO.
- Technical capability to detect attacks for unauthorized access.
- Coordination between and cross education among distributed incident response teams.
- Establishment of continuous monitoring of state information systems by implementing appropriate IT compliance monitoring software.

7f. Security Training & Awareness

Description of Function

The Security Training and Awareness function would develop an information security and privacy awareness and training program for State government. The awareness programs are intended to raise security and privacy awareness in all State personnel and to empower them to understand their role in protecting State information resources and citizen privacy. The training program will introduce security personnel to the State's security standards and recommend best practices for implementing those standards.

An effective security awareness and training program explains proper rules of behavior for the use of agency information technology systems and information. The program communicates security policies and procedures that need to be followed. This must precede and lay the foundation for any sanctions imposed due to non-compliance. Through awareness and training, users first should be

informed of the expectations. Accountability must be derived from a fully informed, well-trained and highly alert workforce.

Rationale and Justification for the Function

Based on recent interviews with Arizona State agency IT management and security personnel, it is evident that agencies have varying levels of awareness about information security risks and mitigation strategies. Since the baseline security standards established by the SISPO require uniform implementation, a single training program can help drive consistency among agencies' security programs.

The SISPO will provide leadership and outreach to focus security and privacy protection awareness throughout State government, but a grassroots acceptance and embrace of this function by State agencies and education within their own organization is essential broad based implementation.

Security training and awareness addresses one of the weakest components of a security program - people. By maintaining a central training platform and conducting regular periodic trainings the enterprise proactively addresses this issue.

Key Activities for this Function

- Inform users of their IT security responsibilities (through awareness and training), as documented in agency security policy and procedures
 - Develop training guidelines for use by operators of State computer systems to educate employees in security awareness and good security practices
- Develop awareness and training materials, and implement the program.
- Garner sufficient funding to implement the agreed-upon strategy.
- Use measurement tools to gauge the success of the program.
- Implement awards and recognition programs for successful implementation in specific agencies. Consult with Arizona Government University (AZGU) on deployment of a security and privacy information training program and repository to ensure routine access to training classes, materials and supplemental information by State employees and contractors.
- Consult with Arizona Government University (AZGU) on deployment of a security and privacy information training program and repository to ensure routine access to training classes, materials and supplemental information by State employees and contractors.

Resource Requirements

The security and privacy training function will require a senior training specialist to develop and deploy a statewide training program (SISPO Phase I).

In addition to a full time training specialist, the function should require a web-based training platform with the appropriate resources to sustain the effort. Most states maintain a separate security and privacy training intranet with the capability to both deliver general training as well as integrate more specific skill training for each agency. The portal will also provide a mechanism to record training delivered to each user of state systems. The status or training will be reported on a quarterly basis to SISPO management.

Critical Success Factors

Critical success factors for security awareness and training include:

- Requiring every new hire to state service to complete baseline security and privacy training prior to granting access to State systems.
- Require all users of State systems to complete annual refresher training. With the speed of advancement of today's technology training materials can become quickly outdated. The key to the success of this function is a rapid refresh and update rate for training curriculum and materials.
- Development of effective partnerships to launch comprehensive awareness campaigns.

8. FUTURE FUNCTIONS

As information technology changes over time and as the security and compliance requirements of organizations evolves, SISPO's roles and responsibilities will need to be reviewed.

The following functions are potential additions to the role of the SISPO to be considered in the future:

- Assist in incorporating cyber security considerations into disaster recovery and business continuity plans
- Assess and audit agencies statewide for disaster recovery capability.
- Ensure security features are included in state critical applications development.
- Assist in and conduct acceptable use violation investigations
- Capture digital forensics and assist law enforcement officials with digital forensics when required
- Provide oversight for Federal Information authentication and personal identity verification compliance between information technology and physical access controls convergence.
- Coordinate and collaborate with external agencies out-side the State such as the; multi-state ISAC, DHS, states CIO, InfraGard and other external entities on statewide cyber-security issues.

“The SISPO would be most helpful in establishing a statewide communications network, interpreting various requirements from federal agencies, and by leading with standards, policies and training.”

**- Denny Brown
CIO, Arizona Public Service**

9. CONCLUSION

It is strongly recommended that the State of Arizona formally establish and fund the SISPO within GITA and allocate the necessary resources to ramp up operations over the next three-year period to systemically lead efforts to reduce cyber security risks.

The office must write and own the Statewide Information Technology Security Strategic Plan and Program and maintain timely compliance oversight with the goal of institutionalizing information security and privacy statewide.

The two new leadership positions needed to ensure success for the SISPO is a Chief Information Security Officer and a Chief Privacy Officer to establish accountability for the program and ensure its success. A.R.S 41-3504 already provides the authority to GITA to adopt security policies and standards but the effective enforcement of those standards requires central oversight of the SISPO.

As shown throughout this document, the success of the office is dependent on the resources allocated to designated functions. These resources will enable the office to facilitate statewide initiatives with agencies. The first phase is critical and should primarily focus on completing a statewide risk assessment and the resulting adjustments to security policies and standards.

The most efficient method of deployment for the SISPO is described below:

Phase/Year	Functional Components	Resources	Key Staff Required
I	<ul style="list-style-type: none"> Security & Privacy Program Development Conduct Statewide Risk Assessment Training and Awareness 	<ul style="list-style-type: none"> ◆ ✓ ◆ 	<ul style="list-style-type: none"> CISO CPO Security Training and Awareness Specialist
II	<ul style="list-style-type: none"> Security & Privacy Program Development Security Standards Oversight Compliance Management Security Analysis and Support Incident Response Oversight Training and Awareness 	<ul style="list-style-type: none"> ✓ ✓ ✓ ◆ ◆ ✓ 	Staff include all key personnel from phase I plus the following staff: <ul style="list-style-type: none"> 2 Security Analysts (1 Senior & 1 Mid-level) 1 Compliance Manager 2 Threat & Vulnerability analyst 1 Incident Response Coordinator 1 Assessment specialist 1 Forensic specialist
III	<ul style="list-style-type: none"> Security & Privacy Program Development Security Standards Oversight Compliance Management Security Analysis and Support Incident Response Oversight Training and Awareness 	<ul style="list-style-type: none"> ✓ ✓ ✓ ✓ ✓ ✓ 	Staff include all key personnel from phase I and II plus the following staff: <ul style="list-style-type: none"> 2 Security Analysts (Mid-level)

✓ = Resources designated for this phase are adequate to accomplish the function

◆ = Resources designated for this phase are adequate to start planning

APPENDIX A: CONSULTANT QUALIFICATIONS and PROJECT METHODOLOGY

Consultant Qualifications

Coalfire Government Systems, LLC (Coalfire), a Coalfire partner company, is an industry leader in developing IT Governance and Compliance Management Solutions in the public and private sectors. Coalfire has either audited information security control effectiveness or provided advisory services for more than 800 organizations located in 30 states and 3 international locations. The company maintains a staff of 30 professionals with industry certifications that include the Certified Information Security Systems Professional® (CISSP®), Certified Information Security Manager® (CISM®), Certified Information Systems Auditor® (CISA®) and Qualified Data Security Professional (QDSP) designation.

In addition to general IT governance and compliance management skills, Coalfire has developed industry expertise in advising State and Local governments on the development of comprehensive information security programs in accordance with best practices outlined in the NIST Special Publications 800 series guidelines. Coalfire applies its best practice-based approach to facilitate enterprise risk assessments, policy development, and IT oversight processes. Coalfire prides itself in the fact that its staff has participated in the development of unified controls frameworks to address emerging and current personal privacy and confidentiality regulations and legislation, such as required by Gramm-Leach-Bliley, Health Insurance Portability and Accountability Act (HIPAA), as well as the U.S.A. Patriot Act.

For this business case analysis, Coalfire has assigned three senior security analysts with specific experience advising other States in the development of security or compliance programs. Each of our executives have planning, operations and forensic investigations experience to help assess alternatives and provide recommendations based upon a solid foundation of similar analysis provided to other State and Local government agencies.

Business Case Methodology

The business case analysis employed on this project integrated local data collection with best practice comparisons to identify strategic organization deficiencies. The process flow identifies the stakeholders, defines goals, reviews policies and guidance, compares and contrasts other states, reviews the high level risks, identifies the gaps and recommends actions.

High-level interviews were conducted in the following organizations to obtain input on both the current status of information security programs and recommendations for program improvement.

- Arizona Department of Corrections (DOC)
- Arizona Department of Economic Security (DES)
- Arizona Department of Transportation (ADOT)
- Arizona Department of Health Services (DHS)
- Arizona Department of Administration (ADOA)
- Arizona Department of Environmental Quality (DEQ)
- Government Information Technology Agency (GITA)
- Auditor General

- Arizona Public Service (APS) (member of ITSAC)
- Office of the Governor
- AZNet

Each of the interviews confirmed that improving state information security programs was indeed justified. The larger entities felt confident that they had adequate resources in both technical skills and funding to protect their information, but they expressed concern about the increasing deployment of shared IT services like AZNet. Each wanted to make sure other agencies maintained consistent controls across the state.

Larger agencies recognized the need to help the smaller, less resourced budget units. These smaller organizations were considered to be at risk and consequently to threaten the larger organizations due to the connected nature of the networks in the State. Additionally there is some concern on being able to maintain the level of technological advancement in hardware, software and personnel skill sets in the State's fiscal environment.

All concurred that more collaboration and cooperation between agencies was needed to mitigate common risks and concerns. All indicated they would support an effort to centralize information security program through a Statewide Information Security and Privacy Office.

APPENDIX B: ACRONYMS AND ABBREVIATIONS

ADOA	Arizona Department of Administration
Auditor General	The State of Arizona Auditor General
AZNet	Arizona's single, privatized, statewide voice and data network outsourced with oversight by the Telecommunications Program Office of the Department of Administration
BOTNET	(ro BOT NET work) Also called a "zombie army," a botnet is a large number of compromised computers that are used to create and send spam or viruses or flood a network with messages as a denial of service attack. The computer is compromised that waits for commands from the person in control of the botnet. There is even a botnet business with lists of compromised computers sold to hackers and spammers.
CIO	Chief Information Officer
CIO Council	Chief Information Officer Council (State of Arizona) – Council of CIOs from major State agencies formed to advise and consult with GITA regarding IT matters.
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
CPO	Chief Privacy Officer
CSI	Computer Security Institute
E-government	Electronic Government
E-mail	Electronic Mail
Executive	The Governor
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FIPS	Federal Information Processing Standards

FISMA	Federal Information Security Management Act of 2002, 44 U.S.C. § 3541, <i>et seq.</i>
FTC	United States Federal Trade Commission
FTE	Full Time Equivalent
FY	Fiscal Year
GAO	Government Accounting Office
GAISP	Generally Accepted Information Security Principles established by the (ISSA)
GITA	Government Information Technology Agency
GLBA	Gramm-Leach-Bliley Act - opened up competition among banks, securities companies and insurance companies allowing for consolidation.
Governor	The Governor of the State of Arizona
HIPAA	Health Insurance Portability and Accountability Act – Title II requires the establishment of national standards for electronic health care transactions. There are provision that addresses the security and privacy of health data.
IA	Information Assurance
ISO	International Standards Organization
ISSA	Information Systems Security Association
IT	Information Technology
ITAC	Information Technology Authority Committee (State of Arizona)
ITSAC	Information Technology Security Advisory Committee was formed to advise GITA on strategic IT security matters
NASCIO	National Association of State Chief Information Officers
NERC	North American Electric Reliability Corporation – is a nonprofit that defines standards for power system operation, monitoring and enforcing compliance with those standards.
NIST	National Institute of Standards and Technology

PIJ	Project Investment Justification – form used by GITA, State of Arizona to approve, disapprove or conditionally approve IT projects over \$25,000 from all State agencies
Risk Management	Risk Management department of ADOA (State of Arizona)
SIPC	State Infrastructure Protection Center – creates or receives computer security alerts and reported intrusions.
SISPO	Statewide Information Security & Privacy Office
SPYBOT	Software modules on your computer or in your browser that are responsible for transmitting information, including computer usage to an external entity.
TISA	Technical Infrastructure Standards Assessment; - agency self-assessment developed by GITA for use by all state agencies to help identify their information technology vulnerabilities and compliance to state standards.
VA	United States Veteran's Administration

APPENDIX C: GLOSSARY OF TERMS

Access	Ability to make use of any information system (IS) resource.
Access control	Refer to logical access control and physical access control.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual authorization to receive specific categories of information.
Availability	Guaranteed service on demand assurance
Best Practice	Is a technique, process, or methodology that, experts agree is appropriate, accepted and widely used, and has proven to reliably lead to a desired result.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
Cyber Security	The computer and information security that is a form of computer science risk management.
Cyber Terror	Is the leveraging of a target's computers and information technology, particularly via the Internet, to cause physical, real-world harm or severe disruption.
Data Integrity	Provides absolute verification that data has not been modified or tampered with.
Efficiency	In this analysis, efficiency includes productivity gains realized from automation, timesavings, and convenience.
E-government	Refers to government's use of information and communication technology to exchange information and services with citizens, businesses, and other arms of government
Encryption	The translation of data into a secret code.
Hardware	The physical equipment used to process programs and data in a cryptographic module.
Hacking	This growing use of the term "hack" is to refer to someone who (sometimes illegally) modifies another program, often a computer game, giving the user access to features otherwise inaccessible to them.
Integrity	Refer to data integrity.
Interface	A logical section of a cryptographic module that defines a set of entry or exit points that provide access to the module, including information flow or physical access.
Interoperability	The ability of software and hardware on different machines from different vendors to share data.
Non-repudiation	The act of assuring the origin and/or issuance of a transaction or action.

Password	A string of characters used to authenticate an identity or to verify access authorization.
Physical access control	Access to buildings and other physical structures.
Portability	Can be carried or moved with ease.
Privacy	State in which data and system access is restricted to the intended user community and target recipient(s).
Private key	A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity and not made public.
Scalability	Refers to how well a hardware or software system can adapt to increased demand.

APPENDIX D: REFERENCES

The following references refer to information that is specific to Arizona or pertinent to this document.



Identity Theft Victims by State (Per 100,000 Population)

January 1 – December 31, 2006

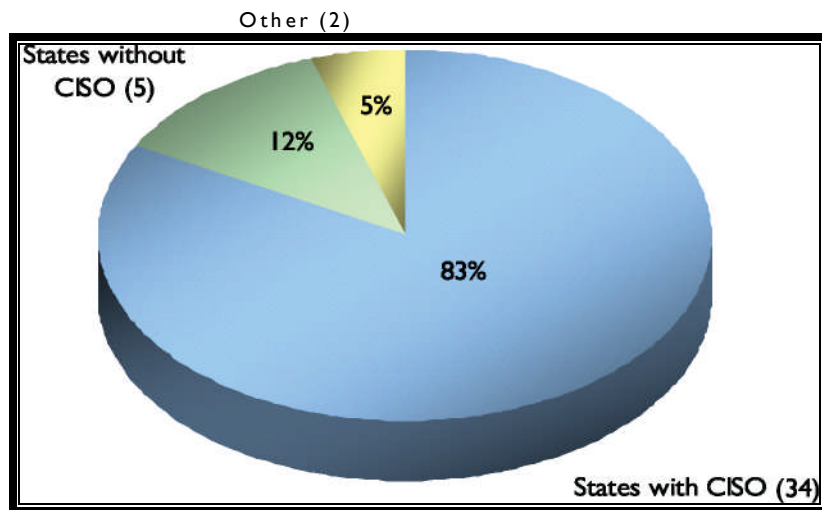
Arizona Number 1.

Victims				Victims			
Rank	Victim State	Per 100,000 Population	Number of Victims	Rank	Victim State	Per 100,000 Population	Number of Victims
1	Arizona	147.8	9,113	26	Tennessee	61.3	3,700
2	Nevada	120.0	2,994	27	Alabama	60.3	2,774
3	California	113.5	41,396	28	Ohio	59.9	6,878
4	Texas	110.6	26,006	29	Kansas	58.8	1,626
5	Florida	98.3	17,780	30	Rhode Island	57.6	615
6	Colorado	92.5	4,395	31	Alaska	57.3	384
7	Georgia	86.3	8,084	32	South Carolina	55.7	2,408
8	New York	85.2	16,452	33	Minnesota	55.6	2,872
9	Washington	83.4	5,336	34	Arkansas	54.7	1,537
10	New Mexico	82.9	1,621	35	Louisiana	52.6	2,256
11	Maryland	82.9	4,656	36	Mississippi	51.3	1,494
12	Illinois	78.6	10,080	37	Nebraska	49.1	868
13	Oregon	76.1	2,815	38	Idaho	49.0	718
14	New Jersey	73.3	6,394	39	Hawaii	47.8	615
15	Virginia	67.2	5,137	40	New Hampshire	46.1	606
16	Michigan	67.2	6,784	41	Montana	45.9	434
17	Delaware	66.7	569	42	Wisconsin	45.6	2,536
18	Connecticut	65.8	2,305	43	Wyoming	42.3	218
19	Pennsylvania	64.9	8,080	44	Kentucky	42.0	1,766
20	North Carolina	64.9	5,748	45	Maine	39.7	525
21	Missouri	64.2	3,753	46	West Virginia	39.3	715
22	Massachusetts	63.7	4,102	47	Iowa	34.9	1,041
23	Oklahoma	63.0	2,254	48	South Dakota	30.2	236
24	Indiana	62.2	3,928	49	North Dakota	29.7	189
25	Utah	61.8	1,577	50	Vermont	28.5	178

A Current View of the State CISO: A National Survey Assessment

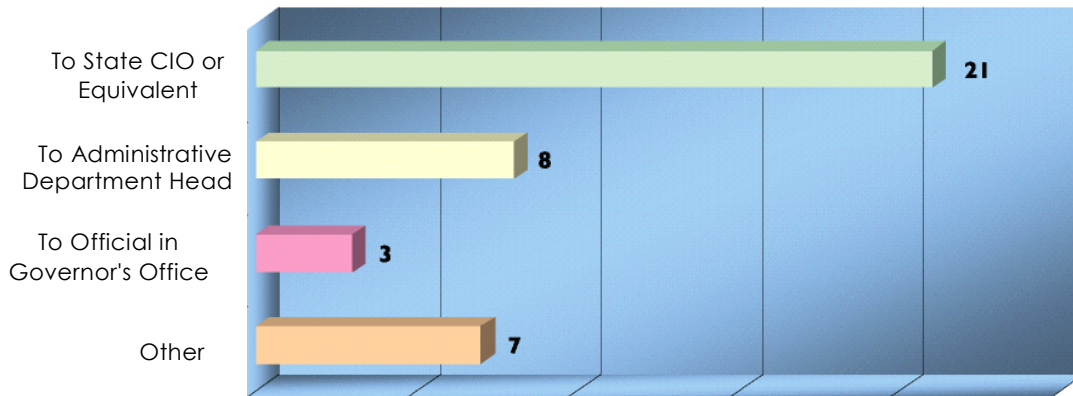
NASCIO September 2006

Figure 2:
Prevalence of the State CISO Role
(41 states responding)



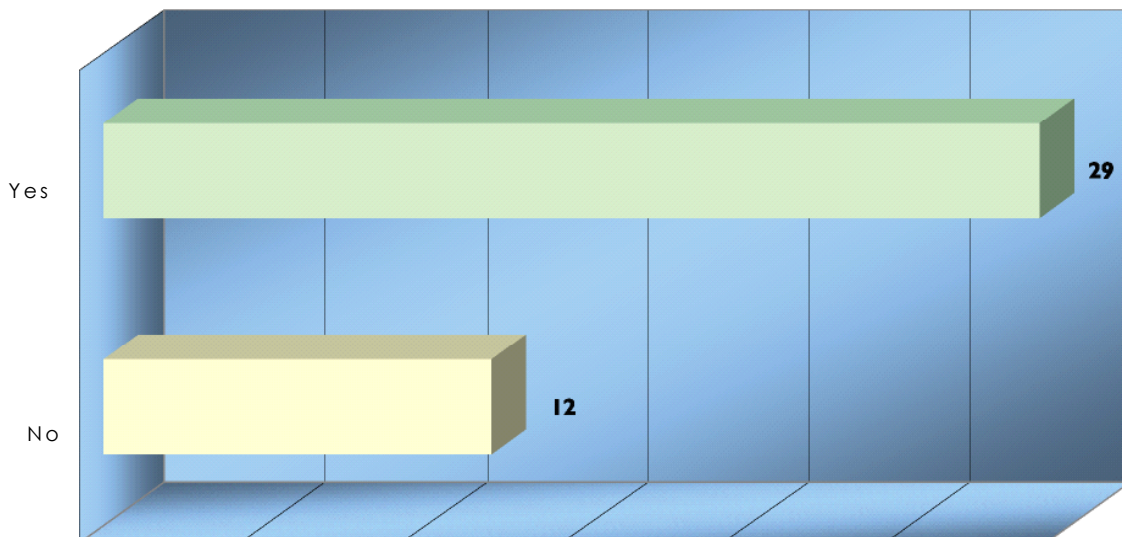
An Evolving IT Security Role:

With eighty-three percent (83%) of responding states confirming that they have a state CISO or the equivalent position, IT security appears to be evolving as a strategic function that must be located at an enterprise level



An Elevated Position

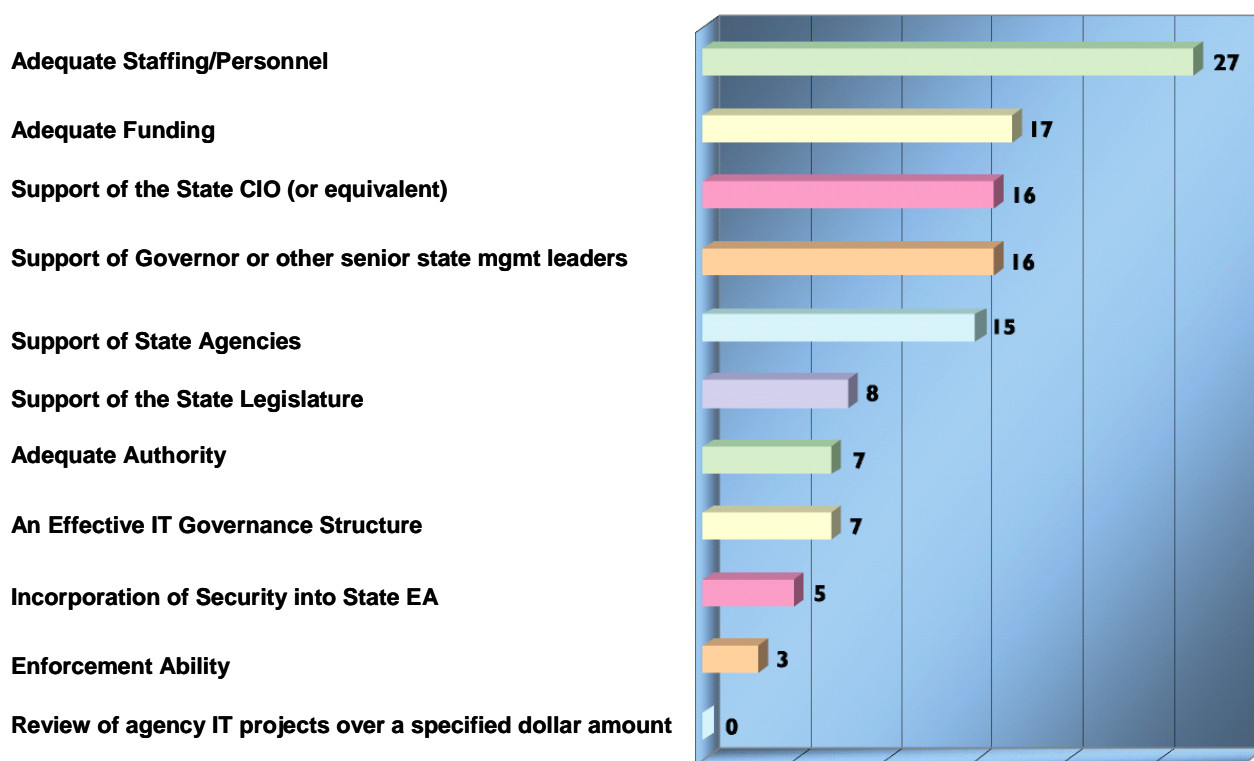
The majority of survey respondents report to the state CIO or equivalent position, while a lesser number report to an administrative department head. Three (3) survey respondents indicated that they report to an official in the Governor's office. The survey results reflect the fact that the state CISO position has risen through the ranks to the upper-levels of state government, giving the state CISO an enterprise-view of IT security. Elevating the position of the state CISO to report to the state CIO or other high-level state government official has necessitated that state CISOs now embrace the importance of establishing relationships with a variety of stakeholders across the state enterprise, such as state homeland security and emergency management officials



A Majority with Enforcement Authority

Over two-thirds of the survey respondents indicated that they have authority to enforce enterprise IT security policies.

What State CISOs Really Need to do their Jobs. Figure 11.



Tier 1 Priorities —The Importance of Adequate Staffing:

The state CISOs were asked to select from a list of 11 items the top three that they needed to do their jobs. According to the responding states, the overwhelming majority of state CISOs need adequate staffing/personnel in order to perform their jobs. The prevalence of this response far exceeded all others.

Tier 2 Priorities—Funding and the Support of Stakeholders:

After adequate staffing, adequate funding is the next most important item followed by the support of the CIO and the support of the Governor or other senior state management leaders in a tie. Close behind those, the state CISOs listed the support of state agencies as a priority. Since sufficient funding is an ever-present necessity, NASCIO published a recent Research Brief on that topic entitled, "*The IT Security Business*

Case: Sustainable Funding to Manage the Risks." Moreover, as the state CISO position is elevated in importance, the value of relationship-building increases as well as the need for support from a variety of stakeholders, including the Governor, CIO and state agency leaders.

Tier 3 Priorities:

The need for the support of the state legislature leads the Tier 3 state CISO priorities. Slightly behind that priority are the need for adequate authority and an effective IT governance structure in a tie. Incorporation of security into a state's enterprise architecture and enforcement ability follow in that descending order. This reflects the fact that the state CISO position is becoming established in many states. Hence, state CISOs now do not have to justify the need for their positions as much as they now have to forge relationships within the state and with external stakeholders in order to carry out their duty to secure state IT systems and infrastructure

Internet guru warns of botnet pandemic

Published: 29 Jan 2007 09:39 GMT

Father of the Internet Vint Cerf has warned high-powered attendees at the World Economic Forum in Davos that the internet is at serious risk from botnets.

Vast networks of compromised PCs, used by criminals for sending spam and spyware and for launching denial of service attacks are reported to be growing at an alarming rate in terms of their potential and Cerf, now an employee of Google, warned they could undermine the future of the internet — likening their spread to a pandemic.

Botnets are getting smaller, more stealthy and more discreet and yet the volumes of spam are going up.

Cerf predicted that a quarter of all PCs currently connected to the internet — around 150 million — could be infected by Trojans which covertly seize control of a computer and its broadband connection, handing control of both to remote criminals.

According to Mark Sunner, chief security analyst at Message Labs, Cerf's words of warning are far from scaremongering and the picture is at least as serious as Cerf paints it.

Sunner said around the turn of the year security experts were watching one botnet, called Spam Thru, which not only had its own antivirus protection to clear other botnets off 'its patch' but had the potential to be 10 times more productive than most other botnets while evading detection because of in-built defenses.

He said the most worrying thing about Spam Thru is that he suspects a major spike in traffic towards the end of 2006 was merely a testing of the waters and much worse could be to come — not least when other similarly sophisticated botnets appear online.

Sunner added: "With new levels of sophistication this has reached a real milestone. Botnets are getting smaller, stealthier and more discreet and yet the volumes of spam are going up.

"Without a hint of scaremongering, will this get a lot worse throughout 2007 in terms of botnet sending? Absolutely, yes."